IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 05-20 E
	)	**HEARING REQUESTED**
DAVID GRAHAM	)	

MOTION TO COMPEL DISCOVERY

AND NOW, comes the defendant, David Graham, by his attorney, Thomas W. Patton, Assistant Federal Public Defender, and files the within Motion to Compel Discovery and in support thereof sets forth as follows:

Mr. Graham is charged with one count of knowingly receiving visual depictions of minors engaging in sexually explicit conduct in violation of Title 18 U.S.C. § 2252(a)(2), and one count of possession of material depicting the sexual exploitation of a minor in violation of Title 18 U.S.C. § 2252(a)(4)(B). The charges stem from a search of Mr. Graham's computer pursuant to a search warrant issued by United States Magistrate Judge Amy Reynolds Hay.

The Department of Homeland Security, United States Immigration and Customs Enforcement (ICE) sent Mr. Graham's work computer to a Pennsylvania State Police laboratory where it was examined by a forensic computer examiner. The forensic computer examiner's examination revealed numerous video files of minors engaging in sexually explicit conduct. Defense counsel requested the opportunity to copy the hard drive taken from Mr. Graham's computer and examined by the State Police. While the government has allowed defense counsel the opportunity to view the video clips at the United States Attorney's office, the government has refused to provide copies of

the hard drive. The United States Attorney's Office has also stated that any computer expert retained by Mr. Graham will be allowed to go to the FBI's office in Pittsburgh and examine the hard drive taken from Mr. Graham's computer at the FBI's office.

The charges Mr. Graham faces create unique and extremely complex defense issues relating to the analysis of the evidence seized. Because of the nature of the charges facing Mr. Graham and the sentencing enhancements possible in this case, defense counsel must determine, for example, whether real or "virtual" minors are contained in the computer memory storage (see 18 U.S.C. § 2256(8)(B)); the possible age of those minors (see 18 U.S.C. § 2252A(c)(2), USSG § 2G2.1(b)(1)); the exact behavior of those minors (see USSG § 2G2.2(b)(3)); whether the computer images traveled in interstate commerce (see discussion infra); when the images were stored in the computer and who had access to the computers at that time; whether the hard drive has been altered; what access the computer operator had to the Internet and with whom he conversed; how computer files were accessed and formatted; and other related technical issues. Such tasks are extremely time-consuming and must be undertaken by a forensic or computer expert. Importantly, any competent computer expert will insist that a computer and other electronically formatted material be viewed "unaltered," i.e. before anyone has gone into the computer and intentionally or unintentionally compromised the status of the computer. The government's refusal to provide Mr. Graham with a copy of the hard drive taken from his computer makes it impossible for defense counsel to effectively perform his task of representing Mr. Graham.

Federal Rule of Criminal Procedure 16 provides in relevant part that

> Upon the request of the defendant the government shall permit the defendant to inspect and copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its

case-in-chief at trial; (iii) the item was obtained from or belongs to the defendant. The information on the hard drive is clearly covered by Rule 16. The hard drive contains data, photographs, and is a tangible object. This information is material to the preparation of the defense, and the government intends to use the information in its case-in-chief. United States v. Hill, 322 F.Supp.2d 1081, 1091 (C.D. Cal. 2004).

Several district courts have ordered the government to provide copies of hard drives to defense counsel subject to stringent protective orders. See Defendant's Exhibit A. Perhaps the best decision explaining the reasoning of these courts is Judge Kozinski's opinion in Hill. Hill involved a defendant charged with possessing child pornography on zip disks who asked the court to compel the government to provide a copy, or "mirror image" of the zip disks. Hill, 322 F.Supp.2d at 1083. The government opposed the motion, arguing that the zip disks contained child pornography and therefore defense counsel and his expert should only be allowed to examine the disks at the local FBI office. Id. at 1091. Judge Kozinski, sitting by designation, rejected the government's argument. First, Judge Kozinski found the cases cited by the government, United States v. Kimbrough, 69 F.3d 723, 730-731 (5th Cir. 1995)(upholding the district court's denial of defendant's motion to compel production of a copy of a video containing child pornography), and United States v. Horn, 187 F.3d 781, 792 (8th Cir. 1999) (upholding the district court's refusal to order the government to produce copies of videos alleged, and later found, to contain child pornography), distinguishable. Id. Judge Kozinski explained that both Kimbrough and Horn "involve appeals from district court decisions denying a defendant's motion to compel production. They do not hold that a district court would abuse its discretion if it were to order the government to produce copies of the materials." Id.

Judge Kozinski went on to find that the defendant would be seriously prejudiced if his expert and counsel did not have copies of the zip disks. Judge Kozinski acknowledged that defense

counsel, through his expert, would have to conduct in-depth analysis of the zip disks to try to determine when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. "The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel and his expert have ready access to the materials that will be the heart of the government's case." Id. at 1092. Judge Kozinski rejected the government's argument that having the disks available for review at the FBI office provided an adequate substitute for copies of the disks. Judge Kozinski realized that the defense expert needed to be able to use his own tools in his own lab to perform his work. Also, the examination of the disks would be a lengthy process requiring multiple trips to the FBI office by the expert who was from a different state. Finally, Judge Kozinski found that there was no reason to believe defense counsel and the defense expert could not be trusted with the material. "Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials." Id. Judge Nancy Gertner of the District of Massachusetts has adopted this analysis. United States v. Fabizio, 341 F.Supp.2d 47, 50 (D.Mass. 2004).

Senior United States District Judge Maurice B. Cohill, Jr. has also agreed that in child pornography cases involving computers it is necessary for an adequate defense that defense counsel be provided with a copy of the hard drive. In both United States v. Oesch, 02-37 E, and United States v. Kuzdzal, 03-12 E, Judge Cohill ordered the government to provide to the undersigned counsel copies of the hard drives involved in each case subject to very stringent protective orders. See Defendant's Exhibit B. In both cases the copies were handled appropriately by defense counsel and his experts with out incident. The same should happen here.

In both Oesch and Kuzdzal, the government relied upon the Fifth Circuit's decision in United

States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995) to support its opposition to providing copies of the hard drives. However, the Hill decision explains why that reliance is unwarranted. Furthermore, the basis for Kimbrough's holding that it was not an abuse of discretion not to provide a copy of the videotape at issue does not withstand scrutiny.

Kimbrough should not be followed for a host of reasons, not the least of which is that its central proposition is nonsensical. Essentially, Kimbrough holds that because child pornography is contraband, it cannot be copied under Rule 16. The court fails to explain why. Apparently, the argument is that contraband cannot be copied by the government or given to defense counsel to possess without violating the law, even under the protection of a court order. By this logic, if the government distributes "child pornography" pictures to a jury during a trial both it and the jurors who receive or possess the pictures are guilty of possessing illegal contraband. Similarly, a defense attorney or investigator who momentarily picks up some seized drugs during Rule 16 discovery would be guilty under the government's logic of possessing illegal drugs. Indeed, a defense expert who obtains samples of drugs to test for the defendant would be guilty of drug possession as well. Obviously, contraband is possessed in the court system on a daily basis, and it is not a crime to make contraband available to a defendant under court direction. The fact that computer images may be contraband says nothing about whether defense counsel can copy them for review and defense preparation.[1] See, Cervantes v. Cates, 76 P.3d 449, 455-456 (Ariz. 2003) (rejecting Kimbrough).

More importantly, there are some very real defense needs which require that the government allow a defendant to copy such material. The starting point of this analysis is the government's own

---

[1]Of course, one of the defense functions is to determine whether the pictures/images are in fact contraband; the government should not be allowed to unilaterally decide that they are, and refuse to allow counsel to examine them with the assistance of an expert in his office or in a laboratory to determine whether they are what the government contends they are.

claims when it comes to examining hard drives. Attached as Defendant's Exhibit C is an Application & Affidavit for Search Warrant sworn to by ICE Agent Sara Seidman seeking a search warrant to allow a search of Mr. Graham's home to seize, and then search, Mr.Graham's computer. In her affidavit, Agent Seidman explains at length the difficulties involved in searching for evidence on computers and the need for the examination to be done in a controlled, laboratory environment. This is an accurate description of the intricacies of searching computer hard drives. Mr. Graham's expert will have to engage in these types of processes to fully explore and develop a defense to the charges in the indictment. The need for a defense expert to examine all of the material in a laboratory or place other than the United States Attorney's Office is obvious. First, it is widely accepted now that computer analysis is a fundamental requirement of any defense effort:

> Computer-based child pornography and obscenity cases require expert witnesses. This is true because of how investigators recover evidence in such cases. The process can be compared technically to the complicated procedures used to analyze urine for drug metabolites. Investigators do not just open a seized computer to find illegal images stashed in the case, they must use a scientific process to recover the evidence that is otherwise undetectable to the unaided human eye. The reports yield a list of files found on a seized computer, the date those files where created, accessed and modified and often include a description of the software and procedures used to extract evidence from the system. Finally, the reports include copies of the evidence investigators discovered in their analysis.

Cox, David: Litigating Child Pornography and Obscenity in the Internet Age, Summer 1999 Journal Technology Law and Policy, 4-SUM J. Tech. L. and Poly 1, at p. 27.

Second, courts have placed demands upon both parties in such cases to determine very technical issues with regard to computer (and photographic/video) evidence. Courts have held, for example, that the government must prove that pornographic images traveled in interstate commerce. See United States v. Hilton, 257 F.3d 50 (1st Cir. 2001); United States v. Henriques, 234 F.3d 263 (5th Cir. 2000); United States v. Wilson, 182 F.3d 737 (10th Cir. 1995). Such an analysis cannot be

undertaken without the use of an expert, and even if such an analysis could be performed at the FBI'S office, it would provide the government with improper work product discovery if it could observe and monitor what a defense expert did in terms of analyzing a seized computer. As for burdens on the defendant, Mr. Graham refers this court to United States v. Campos, 221 F.3d 1143 (10th Cir. 2000), where the defendant sought to challenge the manner in which the government searched the defendant's computer. The court denied the defendant's motion in part because "Mr. Campos offered no evidence as to the methods used by the officers in searching through his computer files." Id. at 47. The clear import of this ruling is that a defendant, through the use of an expert, must examine how a computer was searched by the government if he plans to challenge a government search.

Yet another reason why discovery is so essential in child pornography cases is that the government must show that the person depicted in a given image was a minor, and that requires a clear image which can be examined by an expert. See United States v. Katz, 178 F.3d 368 (5th Cir. 1999) (district court properly suppressed photographic evidence at trial due to failure to provide clear images to defendant during discovery). Such an image must be developed from the source, and the defendant must be allowed to use an expert to evaluate any images to determine whether a challenge may be raised to the government's claim that a minor is in fact depicted. Again, counsel should not be required to visit the United States Attorney's Office with his expert at the government's convenience to conduct appropriate tests and analysis.

The government's legitimate concerns regarding the distribution of child pornography can be addressed in this case through the use of a protective order. District Courts in this and other judicial districts have routinely allowed production of electronic media alleged to contain child pornography to defense counsel pursuant to protective orders. Judge Cohill's and other Court's

protective orders authorizing the production of alleged child pornography to defense counsel are attached as Defendant's Exhibits A and B. Mr. Graham has attached a proposed protective order with this motion. Defense counsel would also note, finally, that as a licensed attorney, member of the bar of this Court, and as an officer of the Court, he would not knowingly allow or facilitate the distribution of child pornography.

Defense counsel has retained the services of GlobalCompuSearch LLC, located in Spokane, Washington to examine the hard drive in this case if the government is ordered to provided a copy to defense counsel. Defense counsel has previously provided the qualifications of GlobalCompuSearch to this Court in both United States v. Kosteniuk, Cr. No. 05-8 E, and United States v. Proctor, Cr. No. 05-2 E. Those qualifications will not be repeated here. Defense counsel has also explained, in those cases, why requiring the defense expert to review the hard drive at the FBI's office is unreasonable. Again, those arguments will not be repeated here.

At bottom, the government's justification for refusing to turn over a copy of the hard drive is based on the argument that defense counsel and his expert can not be trusted to handle this sensitive material. The government has never provided any evidence that GlobalCompuSearch or defense counsel can not be trusted to handle alleged child pornography and, therefore, this Court's findings that defense counsel and his expert can not be trusted with this evidence in the Kosteniuk and Proctor cases are unsupported by any facts. A ruling by this Court that prosecutors can be trusted with sensitive evidence but criminal defense attorneys can not, sends the message that criminal defense attorneys and the experts that work for them are second class citizens. Such a ruling perpetuates a mistaken notion that prosecutors are the "good guys" and that criminal defense attorneys and those who work with them are the "bad guys" doing whatever it takes, ethical or not, to get guilty defendants off the hook.

WHEREFORE, the defendant, David Graham, respectfully requests that this Honorable Court compel the government to provide the requested discovery to the defendant for inspection and copying.

Respectfully submitted,

/s/ Thomas W. Patton
Thomas W. Patton
Assistant Federal Public Defender
PA I.D. No. 88653